PhishMe Reporter™

RZECZYWISTE ZAGROŻENIA W CZASIE RZECZYWISTYM ZGŁASZANE PRZEZ PRACOWNIKÓW

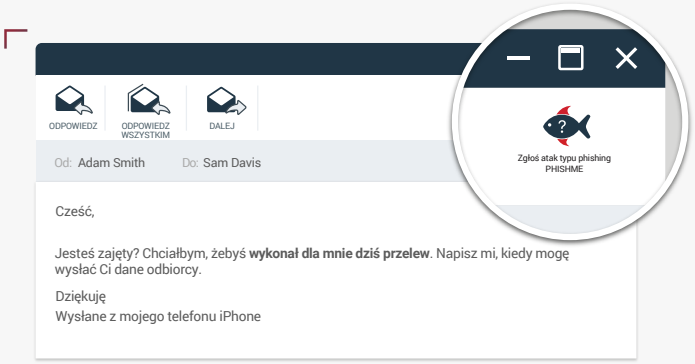
Mimo że PhishMe Simulator uczy pracowników, jak ustrzec się przed próbami phishingu, samo „nieklikanie” łączy nie wystarczy. Podczas ataku typu phishing liczy się wczesne wykrycie. Widoczność zagrożenia jest ważna dla zespołów ds. bezpieczeństwa operacji i reagowania na zdarzenia, aby mogły one maksymalnie skrócić czas dostępu atakującego do Twojej sieci. PhishMe Reporter™ to proste i oszczędne narzędzie dla organizacji, umożliwiające zgłaszanie przez użytkowników podejrzanych wiadomości e-mail, które mogą być pierwszym etapem ataku cybernetycznego.

Dlaczego warto wybrać PhishMe Reporter™?

Udowodniono, że program PhishMe zmniejsza ryzyko związane z zaawansowanymi atakami cybernetycznymi ukierunkowanymi na pracowników o nawet 95% – to Twoja ostateczna broń przeciwko niebezpiecznym próbom phishingu.

Najważniejsze korzyści

- Standaryzacja i organizacja procesu raportowania przez użytkowników
- Szybsze wykrywanie i reagowanie na ataki z wykorzystaniem poczty elektronicznej za pomocą raportów generowanych przez użytkownika
- Analiza adresów URL i załączników typu malware z wykorzystaniem rozwiązań firm zewnętrznych
- Zminimalizowanie konsekwencji naruszeń dzięki aktywnemu reagowaniu i większej widoczności
- Edytowalne informacje zwrotne od użytkowników zachęcają pracowników do włączenia się w proces zapewniania bezpieczeństwa



Co to jest PhishMe Reporter™?

Gdy rozwiązania techniczne, takie jak filtrowanie proxy, przepisywanie adresów URL czy DLP zawiodą, użytkownicy są ostatnią linią obrony. Odpowiednio przeszkoleni użytkownicy mogą łatwo i we właściwym czasie przekazywać cenne informacje na temat zagrożeń, rozpoznając i raportując podejrzane wiadomości e-mail. Organizacje nie wykorzystują tych możliwości i w konsekwencji pozwalają na tygodnie, a nawet miesiące szkodliwej działalności w sieci.

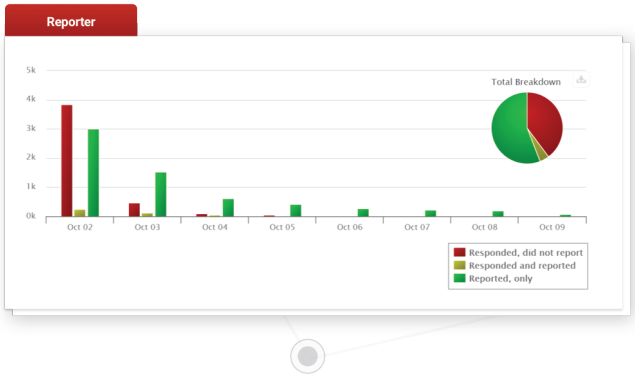
PhishMe Reporter usprawnia proces raportowania poprzez instalację dodatku e-mail na pasku narzędzi poczty elektronicznej użytkowników. Po jego kliknięciu podejrzana wiadomość e-mail jest przekazywana do zespołu wraz z informacjami potrzebnymi do analizy i reagowania na zagrożenie.

Reporter automatycznie odróżnia wiadomości e-mail pochodzące ze scenariuszy programu PhishMe Simulator od wiadomości zgłoszonych z nieznanych źródeł, dzięki czemu tylko raporty dotyczące potencjalnych szkodliwych wiadomości e-mail są przesyłane w celu analizy do odpowiednich zespołów ds. bezpieczeństwa lub do PhishMe Triage.

Usprawnione raportowanie

Niezależnie od stosowanych procedur raportowania, program Reporter może pomóc w ich ulepszeniu poprzez:

- Zachowywanie pełnych nagłówków zgłoszonych wiadomości e-mail, co pozwala na blokowanie i usuwanie podobnych wiadomości.
- Uwzględnianie w raporcie wszelkich załączników i adresów URL.
- Uzupełnianie kampanii programu Simulator, monitorowanie reakcji użytkowników i czasu reakcji ze strony organizacji.



Czy ten e-mail to scenariusz PhishMe?

TAK.

?

▼

ZAREJESTRUJ ZGŁOSZENIE OD UŻYTKOWNIKA W PHISHME

▼

WYŚWIETL PODZIĘKOWANIE DLA UŻYTKOWNIKA

KLIK!

„Co się stanie, jeśli kliknę ten przycisk…?”

NIE, TO PRAWDZIWA WIADOMOŚĆ.

?

▼

ZGŁOŚ E-MAIL DO ZESPOŁU DS. REAGOWANIA

▼

WYŚWIETL PODZIĘKOWANIE DLA UŻYTKOWNIKA

▼

WYŚLIJ DO TRIAGE LUB WEWNĘTRZNEGO ZESPOŁU DS. BEZPIECZEŃSTWA W CELU PRZEPROWADZENIA ANALIZY ORAZ OKREŚLENIA DALSZYCH DZIAŁAŃ.

Wiadomości e-mail PhishMe Simulator

Program Reporter gromadzi zgłoszenia wiadomości e-mail wysłanych przez program Simulator, sprawdza, którzy użytkownicy wysłali te raporty i przesyła im podziękowanie wraz z informacją o pomyślnym wysłaniu raportu. Pozytywne informacje zwrotne dodatkowo zwiększają możliwości pracowników dotyczące skutecznej identyfikacji ataków cybernetycznych. Wszystkie tego typu informacje są monitorowane i uwzględniane w statystykach zgłoszeń w ramach rozwiązania PhishMe.

Podejrzane wiadomości e-mail od nieznanego nadawcy

Zgłoszenia dotyczące podejrzanych wiadomości e-mail od nieznanego nadawcy są przekazywane do określonej lokalizacji lub do Triage, gdzie są analizowane przez wewnętrzny zespół ds. bezpieczeństwa organizacji. Podejrzane wiadomości e-mail są przesyłane w załączniku wraz z oryginalnym nagłówkiem i informacjami kontekstowymi umożliwiającymi szybką analizę. Zespoły ds. bezpieczeństwa operacji i reagowania na zdarzenia mogą ustalać priorytety analizy między innymi na podstawie skuteczności użytkowników w zakresie identyfikacji prób phishingu w przypadku korzystania z Triage.

PhishMe jest wiodącym dostawcą rozwiązań obrony przed phishingiem dla organizacji obawiających się najpopularniejszego obecnie rodzaju ataku — spear phishing. Opierająca się na informacjach platforma PhishMe zamienia pracowników w aktywną linię obrony umożliwiając im identyfikowanie, zgłaszanie i zapobieganie atakom typu spear phishing i „drive-by” oraz wykorzystującym złośliwe oprogramowanie. Nasze otwarte podejście umożliwia łatwą integrację PhishMe z systemami zabezpieczeń, co zapewnia widoczne usprawnienie procesu decyzyjnego organizacji w kwestii bezpieczeństwa. Klienci PhishMe należą do przemysłów obronnego, produkcyjnego i energetycznego, branży usług finansowych oraz opieki zdrowotnej. Poza tym, naszymi klientami jest 1000 globalnych organizacji, które zrozumiały, że zmiana zachowań użytkowników pozwoli poprawić bezpieczeństwo i reakcje na wydarzenia oraz zmniejszyć ryzyko narażenia.

PHISHME

Więcej informacji:

Strona: phishme.com/contact Tel.: 703 652 0717
Adres: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175